ارائه چارچوب مدیریت امنیت شبکه در سازمان ها

محمد کریم نیری
کارشناس ارشد شبکه های کامپیوتری – دانشگاه یزد
mknayeri@gmail.com

چکیده

داده ها و یا اطلاعات دارای نقشی اساسی برای سازمان ها در عصر حاضر می باشند. اهمیت این موضوع به حدی است که عصر حاضر را عصر اطلاعات نامیده اند. صیانت از اطلاعات حساس موجود بر روی هر کامپیوتر وظیفه ای مهم برای هر کاربر کامپیوتر است. دستیابی و استفاده از داده های حساس توسط افراد غیرمجاز مهمترین تهدید امنیتی در حال حاضر است که می بایست همواره نسبت به آن حساسیت خاصی را داشت.

در این مقاله کوشش شده است تا رویکردی لایه بندی شده برای امن سازی شبکه به شما معرفی گردد. این رویکرد هم یک استراتژی تکنیکی است که ابزار و امکان مناسبی را در سطوح مختلف در زیرساختار شبکه شما قرار می دهد و هم یک استراتژی سازمانی است که مشارکت همه از هیأت مدیره تا قسمت فروش را می طلبد. هدف در اینجا ایجاد درکی در سطح پایه از امنیت شبکه و پیشنهاد یک رویکرد عملی مناسب برای محافظت از دارایی های دیجیتال است. بعلاوه، با رویکرد عملی که در اینجا معرفی می شود، می توانید بدون هزینه کردن بودجه های کلان، موانع موثری بر سر راه اخلال گران امنیتی ایجاد کنید.

کلمات کلیدی: مدیریت، امنیت، سازمان، شبکه

۱. مقدمه

در دنیایی که وجه مشخصه آن فناوری سطح بالا و ارتباطات گسترده می باشد، هر سازمانی نیاز به سیاست های امنیتی که مدبرانه تدوین شده باشند، دارد. هدف سیاست های امنیتی تعریف چارچوبی از روال ها، راهنماها و تمریناتی است که امنیت را در محیط سازمان برقرار و مدیریت می نماید. با اجرای دقیق سیاست های امنیتی، سازمان ها می توانند تهدیدات را کاهش دهند. به سیاست امنیتی به عنوان یک سند زنده نگریسته می شود، بدین معنا که فرایند تکمیل و اصلاح آن هیچ گاه متوقف نشده، متناسب با تغییر فناوری و نیازهای کاربران به روز می شود.

برای تدوین سیا ست امنیتی پس از تحلیل ریـ سک های سازمان، می توان به روش هایی که دیگران برگزیده اند متو سل شد.[۱ تا ۴] معمولا تجارب مفیدی که قبلا در صنایع مشابه انجام شده و نتایج خوبی از آنها نتیجه شده است به صورت عمومی گزارش شده و در قالب مقالات تخصصی ارائه می گردند.[۵ و ۶] استانداردهای شناخته شده ای نیز برای این کار وجود دارد که می توان از آنها هم بهره گرفت.[۷ تا ۹]

بـ سیاری از شرکت های تجاری بر این باورند که خرید تجهیزات کافی، می توانند ایجاد زیر ساخت امنی را برای آن ها ایجا کند. فایروال ها، سیستم های تشخیص نفوذ، برنامه آنتی ویروس، و محصولات احراز هویتی چند فاکتوری تنها برخی از ابزارهای موجود برای کمک به حفاظت از شبکه و داده های آن می باشد. مهم است که به خاطر داشته باشیم که هیچ محصول یا ترکیبی از محصولات به خودی خود باعث ایجاد یک سازمان امن نخواهد شد. امنیت یک فرایند است. هیچ ابزاری وجود ندارد که شما آن را نصب کرده و خیالتان را راحت کنید.

امنیت ایجاد شده توسط کلیه محصولات امنیتی تنها به مقداری است که افراد آن را پیکربندی و حفظ نموده اند. خرید و اجرای محصولات امنیتی تنها باید در صدی از بودجه امنیتی را به خود اختصاص دهد. کارکنانی که وظیفه حفظ امنیت شبکه را بر عهده دارند باید به اندازه کافی، آموزش، و مهارت بکار گرفتن محصولات امنیتی را در شبکه داشته باشند تا بتوانند از آن ها درست و بموقع استفاده کنند. متاسفانه، در بسیاری از سازمان ها فعالیت های امنیتی نادیده گرفته شده و یا تنها برای حمایت از فعالیت های جاری سازمان بکار می رود.

برای بسیاری از سازمان ها، هزینه ایجاد یک وضعیت امنیتی قوی به عنوان عنصر منفی و زیانبار تلقی می شود، همانند هزینه ای که برای بیمه صرف می شود. سازمان تمایلی به صرف پول در این زمینه ندارد، اما خطرات هزینه نکردن در این زمینه به ریسک آن نمی ارزد. مشکلی که این واقعیت را تشدید کرده این است که متخصصان فناوری اطلاعات با زبانی متفاوت از زبان مدیریت صحبت می کنند. متخصصان فناوری اطلاعات به طور کلی پیرامون فن آوری متمرکز می شوند حال آنکه مدیریت بر درآمدزایی و کاهش هزینه ها تمرکز دارد. این امر می تواند مفید باشد اگر مدیریت گام هایی برای یادگیری برخی از اصول فن آوری اطلاعات بردارد، متخصصان فناوری اطلاعات نیز باید ابتکار عمل را در یادگیری و بکارگیری برخی از مفاهیم کسب و کار بکار ببندند. یادگیری این مفاهیم به نفع سازمان خواهد بود زیرا زیر ساخت های فنی می توانند مقرون به صرفه اجرا شوند.[۱۰]

۲. رویکرد امنیتی لایه بندی شده

در این قسمت رویکردی لایه بندی شده برای امن سازی شبکه به شما معرفی می گردد. این رویکرد هم یک استراتژی تکنیکی است که ابزار و امکان مناسبی را در سطوح مختلف در زیرساختار شبکه شما قرار می دهد و هم یک استراتژی سازمانی است که مشارکت همه از هیأت مدیره تا قسمت فروش را می طلبد.[۱۱]

رویکرد امنیتی لایه بندی شده روی نگهداری ابزارها و سیستمهای امنیتی و روال ها در پنج لایه مختلف در محیط فناوری اطلاعات متمرکز می گردد:

- محیط پیرامون
- شبکه
- میزبان[۱]
- برنامه کاربردی
- داده

هدف در اینجا ایجاد درکی در سطح پایه از امنیت شبکه و پیشنهاد یک رویکرد عملی مناسب برای محافظت از دارایی های دیجیتال است. محافظت از اطلاعات اختصاصی به منابع مالی نامحدود و عجیب و غریب نیاز ندارد. با درکی کلی از مسأله، خلق یک طرح امنیتی استراتژیکی و تاکتیکی می تواند تمرینی آسان باشد .بعلاوه، با رویکرد عملی که در اینجا معرفی می شود، می توانید بدون هزینه کردن بودجه های کلان، موانع موثری بر سر راه اخلال گران امنیتی ایجاد کنید.

۳. افزایش ضریب عملکرد هکرها

متخصصان امنیت شبکه از اصطلاحی با عنوان ضریب عملکرد استفاده می کنند که مفهومی مهم در پیاده سازی امنیت لایه بندی است .ضریب عملکرد بعنوان میزان تلاش مورد نیاز توسط یک نفوذگر بمنظور تحت تأثیر قراردادن یک یا بیشتر از یکی از سیستم ها و ابزار امنیتی تعریف می شود که باعث رخنه کردن در شبکه می شود. یک شبکه با ضریب عملکرد بالا به سختی

[۱] Host

مورد د ستبرد قرار می گیرد در حالیکه یک شبکه با ضریب عملکرد پایین می تواند نسبتاً به راحتی مختل شود .اگر هکرها تشخیص دهند که شبکه شما ضریب عملکرد بالایی دارد، که فایده رویکرد لایه بندی شده نیز هست، احتمالاً شبکه شما را رها می کنند و به سراغ شبکه هایی با امنیت پایین تر می روند و این دقیقاً همان چیزیست که شما می خواهید.

برای رسیدن به شبکه ای با ضریب عملکرد بالا باید شبکه تان را ارزیابی کنید – چگونگی استفاده از آن، طبیعت داده های ذخیره شده، کسانی که نیاز به دسترسی دارند، نرخ رشد آن و غیره – و سپس ترکیبی از سیستم های امنیتی را که بالاترین سطح محافظت را ایجاد می کنند، با توجه به منابع در دسترس پیاده سازی کنید.

۴. مدل امنیت لایه بندی شده

در **Error! Reference source not found.** مدل امنیت لایه بندی شده و بعضی از تکنولوژی هایی که در هر سطح مورد استفاده قرار می گیرند، ارائه شده اند. در ادامه این تکنولوژی ها مورد بررسی قرار خواهند گرفت.

لایه های امنیتی	ابزار های قابل استفاده
محیط پیرامون	دیواره آتش آنتی ویروس های شبکه ای رمزنگاری شبکه خصوصی مجازی
شبکه	سیستم تشخیص/جلوگیری از نفوذ سیستم مدیریت آسیب احراز هویت کنترل دسترسی
میزبان	سیستم تشخیص نفوذ میزبان سیستم ارزیابی آسیب پذیری میزبان آنتی ویروس کنترل دسترسی/ تایید هویت کاربر
برنامه کاربردی	سیستم تشخیص نفوذ میزبان سیستم ارزیابی آسیب پذیری میزبان

	کنترل دسترسی/ تایید هویت کاربر تعیین صحت ورودی
داده	رمزنگاری کنترل دسترسی/ تایید هویت کاربر

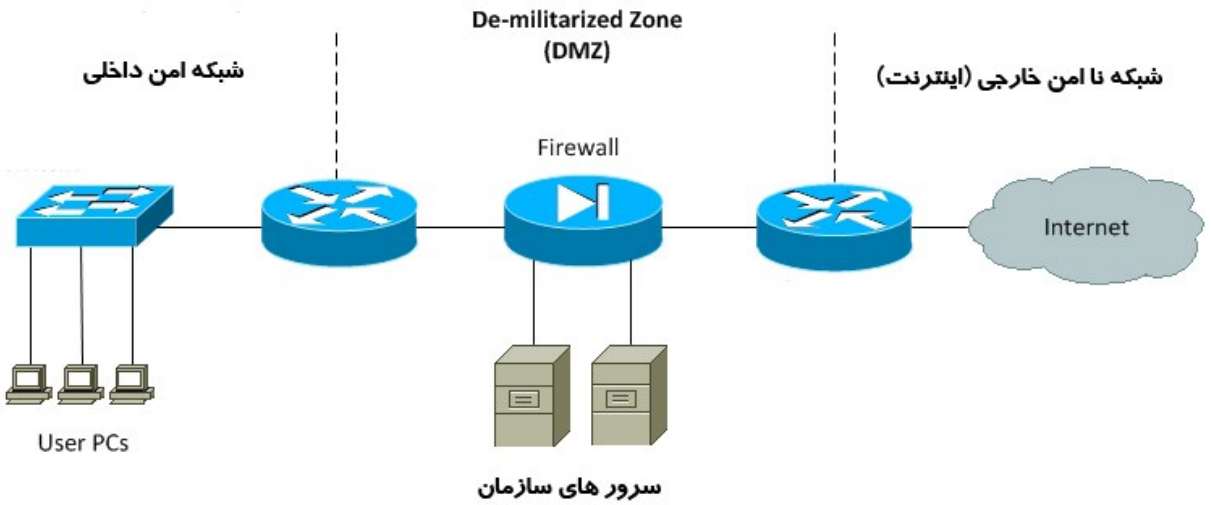
جدول ۱

۵. سطح ۱ : محیط پیرامون

منظور از پیرامون، اولین خط دفاعی نسبت به بیرون و به عبارتی به شبکه غیرقابل اعتماد است. «پیرامون» اولین و آخرین نقطه تماس برای دفاع امنیتی محافظت کننده شبکه است. این ناحیه ای است که شبکه به پایان می رسد و اینترنت آغاز می شود. پیرامون شامل یک یا چند فایروال و مجموعه ای از سرورهای به شدت کنترل شده است که در بخشی از پیرامون قرار دارند و بعنوان DMZ[۱] شناخته می شوند.

DMZ معمولاً وب سرورها، مدخل ایمیل ها، آنتی ویروس شبکه و سرورهای DNS را دربرمی گیرد که باید در معرض اینترنت قرار گیرند. فایروال قوانین سفت و سختی در مورد اینکه چه چیزی می تواند وارد شبکه شود و چگونه سرورها می توانند با اینترنت و شبکه داخلی تعامل داشته باشند، دارد. پیرامون شبکه، به اختصار، دروازه شما به دنیای بیرون و برعکس، مدخل دنیای بیرون به شبکه شماست.

تصویر ۱ بیانگر این ناحیه در یک سناریوی ساده از شبکه یک سازمان می باشد.



تصویر ۱: تصویر DMZ

[۱] Demilitarized zone

۵-۱ . دیواره آتش

معمولاً یک فایروال روی سروری نصب می گردد که از یک طرف به شبکه ناامن خارجی و از سوی دیگر به شبکه امن داخلی متصل است. فایروال سه عمل اصلی انجام می دهد:

- کنترل ترافیک
- تبدیل آدرس
- نقطه پایانی VPN

فایروال کنترل ترافیک را با سنجیدن مبداء و مقصد تمام ترافیک وارد شونده و خارج شونده انجام می دهد و تضمین می کند که تنها تقاضاهای مجاز اجازه عبور دارند. بعلاوه، فایروال ها به شبکه امن در تبدیل آدرس های IP داخلی به آدرس های قابل رویت در اینترنت کمک می کنند. این کار از افشا اطلاعات مهم درباره ساختار شبکه تحت پوشش فایروال جلوگیری می کند. یک فایروال همچنین می تواند به عنوان نقطه پایانی تونل های VPN (که بعدا بیشتر توضیح داده خواهد شد) عمل کند. این سه قابلیت فایروال را تبدیل به بخشی واجب برای امنیت شبکه شما می کند.

۵-۲. آنتی ویروس شبکه

این نرم افزار در DMZ نصب می شود و محتوای ایمیل های وارد شونده و خارج شونده را با پایگاه داده ای از مشخصات ویروس های شناخته شده مقایسه می کند. این آنتی ویروس ها آمد و شد ایمیل های آلوده را مسدود می کنند و آنها را قرنطینه می کنند و سپس به دریافت کنندگان و مدیران شبکه اطلاع می دهند. این عمل از ورود و انتشار یک ایمیل آلوده به ویروس در شبکه جلوگیری می کند و جلوی گسترش ویروس توسط شبکه شما را می گیرد. آنتی ویروس شبکه، مکملی برای حفاظت ضدویروسی است که در سرور ایمیل شما و کامپیوترهای مجزا صورت می گیرد. بمنظور کارکرد مؤثر، دیتابیس ویروس های شناخته شده باید به روز نگه داشته شود.

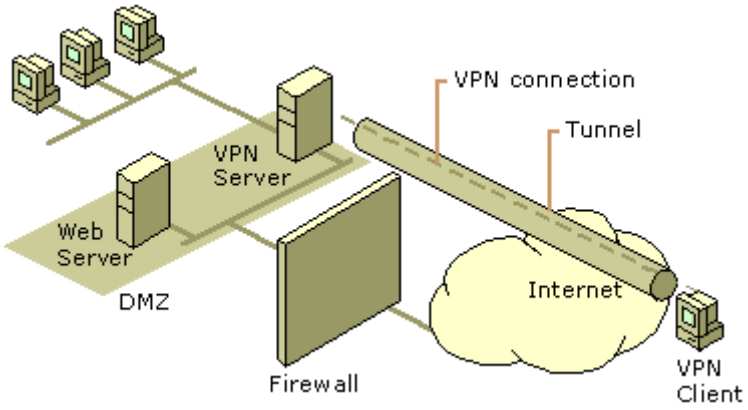
۵-۳. VPN[۱]

یک شبکه اختصاصی مجازی(VPN) از رمزنگاری سطح بالا برای ایجاد ارتباط امن بین ابزار دور از یکدیگر، مانند لپ تاپ ها و شبکه مقصد استفاده می کند. شبکه اختصاصی مجازی اساساً یک تونل رمزشده، تقریباً با امنیت و محرمانگی یک شبکه اختصاصی، اما از میان اینترنت است.

وی‌پی‌ان دو رایانه یا دو شبکه را به کمک یک شبکه دیگر که به عنوان مسیر انتقال به کار می‌گیرد به هم متصل می‌کند. برای نمونه می‌توان دو رایانه یکی در تهران، و دیگری در مشهد که در فضای اینترنت به یک شبکه و صل شده‌اند ا شاره کرد. وی‌پی‌ان از نگاه کاربر کاملاً مانند یک شبکه محلی به نظر می‌رسد. برای پیاده سازی چنین چیزی، وی‌پی‌ان به هر کاربر یک آدرس آی‌پی مجازی می‌دهد. داده‌هایی که روی این ارتباط آمد وشد دارند را سرویس‌دهنده نخست به رمز در آورده و در قالب بسته‌ها بسته‌بندی کرده و به سوی سرویس‌گیرنده وی‌پی‌ان می‌فرستد. سرویس گیرنده وی‌پی‌ان بسته هارا پس از دریافت رمز گشایی کرده و پردازش لازم را روی آن انجام می‌دهد.

[۱] Virtual Private Network

این تونل در یک مسیریاب بر پایه VPN ، فایروال یا یک سرور در ناحیه DMZ پایان پذیرد. برقراری ارتباطات VPN برای تمامی بخش های دور و بی سیم شبکه یک عمل مهم است که نسبتاً آسان و ارزان پیاده سازی می شود. تصویر ۲ این تکنولوژی را نمایش می دهد.



تصویر ۲: VPN

۴-۵. مزایا ، معایب و ملاحظات سطح پیرامون شبکه

تکنولوژی های ایجاد شده سطح پیرامون شبکه سال ها ست که در د سترس ه ستند، و بی شتر خبرگان IT با تواناییها و نیازهای عملیاتی آنها به خوبی آشنایی دارند. بنابراین، از نظر پیاده سازی آسان و توأم با توجیه اقتصادی هستند.

اما از آنجا که بیشتر این سیستم ها تقریباً پایه ای هستند و مدت هاست که در دسترس بوده اند، بیشتر هکرهای پیشرفته روش هایی برای دور زدن آنها نشان داده اند. برای مثال، یک ابزار آنتی ویروس نمی تواند ویروسی را شناسایی کند مگر اینکه از قبل علامت شناسایی ویروس را در دیتابیس خود داشته باشد و این ویروس داخل یک فایل رمز شده قرار نداشته باشد. اگرچه وی پی ان رمزنگاری موثری را ارائه می کند، اما کار اجرایی بی شتری را برروی کارمندان IT تحمیل می کنند، چرا که کلیدهای رمزنگاری و گروه های کاربری باید بصورت مداوم مدیریت شوند.

پیچیدگی معماری شبکه شما می تواند تأثیر قابل ملاحظه ای روی میزان اثر این تکنولوژی ها داشته باشد. برای مثال، ارتباطات چندتایی به خارج احتمالاً نیاز به چند فایروال و آنتی ویروس خواهد داشت. معماری شبکه بطوری که تمام این ارتباطات به ناحیه مشترکی ختم شود، به هرکدام از تکنولوژی های مذکور اجازه می دهد که به تنهایی پوشش مؤثری برای شبکه ایجاد کنند.

انواع ابزاری که در DMZ شما قرار داند نیز یک فاکتور مهم است. این ابزار ها چه میزان اهمیت برای کسب و کار شما دارند؟ هرچه اهمیت بیشتر باشد، معیارها و سیاست های امنیتی سفت و سخت تری باید این ابزارها را مدیریت کنند.

۶.سطح ۲ : امنیت شبکه

سطح شبکه در مدل امنیت لایه بندی شده به شبکه داخلی شما اشاره دارد. شبکه داخلی شما ممکن است شامل چند کامپیوتر و سرور و یا شاید پیچیده تر یعنی شامل اتصالات نقطه به نقطه به دفترهای کار دور باشد. بیشتر شبکه های امروزی باز هستند؛ یعنی هنگامی که داخل شبکه قرار دارید، می توانید به راحتی درمیان شبکه حرکت کنید. این قضیه بخصوص برای

سازمان های کوچک تا متوسط صدق می کند که به این ترتیب این شبکه ها برای هکرها و افراد بداندیش دیگر به اهدافی وسوسه انگیز مبدل می شوند.تکنولوژی های ذیل امنیت را درسطح شبکه برقرارمی کنند:

سیستم تشخیص نفوذ (IDS) و سیستم جلوگیری از نفوذ (IPS)

تکنولوژی های IDS [۱] و IPS [۲] ترافیک گذرنده از شبکه شما را با جزئیات بیشتر نسبت به فایروال تحلیل می کنند. مشابه سیستم های آنتی ویروس، ابزارهای IDS و IPS ترافیک را تحلیل و هر بسته اطلاعات را با پایگاه داده ای از مشخصات حملات شناخته شده مقایسه می کنند. هنگامی که حملات تشخیص داده شوند، این ابزار وارد عمل می شوند. ابزارهای IDS مسئولین IT را از وقوع یک حمله مطلع می سازند. ابزارهای IPS یک گام جلوتر می روند و بصورت خودکار ترافیک آسیب رسان را مسدود می کنند.

در این سلسله مباحث، به کنترل دسترسی [۳] و تأیید هویت [۴] در سطوح شبکه، میزبان، نرم افزار و دیتا در چارچوب امنیتی لایه بندی شده می پردازیم. میان طرح های کنترل دسترسی بین لایه های مختلف همپوشانی قابل توجهی وجود دارد. معمولاً تراکنش های تأیید هویت در مقابل دید کاربر اتفاق می افتد .اما به خاطر دا شته با شید که کنترل د ستر سی و تأیید هویت مراحل پیچیده ای هستند که برای ایجاد بیشترین میزان امنیت در شبکه، باید به دقت مدیریت شوند.

کنترل دسترسی نیازمند تأیید هویت کاربرانی است که به شبکه شما دسترسی دارند .هم کاربران و هم ابزارها باید با ابزار کنترل دسترسی در سطح شبکه کنترل شوند.

۶-۲. مزایا، معایب و ملاحظات لایه شبکه

تکنولوژی های IPS، IDS و مدیریت آسیب پذیری تحلیل های پیچیده ای روی تهدیدها و آسیب پذیری های شبکه انجام می دهند. در حالیکه فایروال به ترافیک، برپایه مقصد نهایی آن اجازه عبور می دهد. ابزار IPS و IDS تجزیه ئ تحلیل عمیق تری را برعهده دارند، و بنابراین سطح بالاتری از محافظت را ارائه می کنند. با این تکنولوژی های پیشرفته، حملاتی که داخل ترافیک قانونی شبکه وجود دارند و می توانند از فایروال عبور کنند، مشخص خواهند شد و قبل از آ سیب ر سانی به آنها خاتمه داده خواهند شد.

در سوی دیگر این نکته قابل توجه است که IDS ها تمایل به تولید تعداد زیادی علائم هشدار غلط دارند، که به عنوان False Positive نیز شناخته می شوند. این بدین معنی است که هنگامی که IDS ممکن است یک حمله را کشف و به اطلاع شما برساند، این اطلاعات می تواند زیر انبوهی از هشدارهای غلط یا دیتای کم ارزش مدفون شود. مدیران IDS ممکن است به سرعت حساسیت خود را نسبت به اطلاعات تولید شده توسط سیستم از دست بدهند. برای تأثیرگذاری بالا، یک IDS باید به طور پیو سته برر سی شود و برای الگوهای مورد ا ستفاده و آ سیب پذیری های کشف شده در محیط شما تنظیم گردد. چنین نگهداری معمولاً میزان بالایی از منابع اجرایی را مصرف می کند.

موفقیت ابزارهای امنیت سطح شبکه به نحوی به سرعت اتصالات داخلی شبکه شما وابسته است. زیرا ابزارهای IDS و IPS ، مدیریت آ سیب پذیری و امنیت کاربر انتهایی ممکن ا ست منابعی از شبکه ای را که از آن محافظت می کنند، م صرف کنند. سرعت های اتصالی بالاتر تأثیر منفی این ابزارها بر کارایی شبکه را به حداقل خواهد ر ساند. در پیاده سازی این تکنولوژی ها شما باید به مصالحه بین امنیت بهبودیافته و سهولت استفاده توجه کنید، زیرا بسیاری از این محصولات برای کارکرد مؤثر باید به طور پیوسته مدیریت شوند و این ممکن است استفاده از آن محصولات را در کل شبکه با زحمت مواجه سازد.

---

[۱] Intrusion Detection System
[۲] Intrusion Preventing System
[۳] Access Control
[۴] Authentication

وقتی که این تکنولوژی ها را در اختیار دارید، بهبود پیوسته شبکه را در خاطر داشته باشید. در شبکه هایی با پویایی و سرعت گسترش بالا، تطبیق با شرایط و ابزار جدید ممکن است مسأله ساز گردد.

۷. سطح ۳: امنیت میزبان

سطح میزبان در مدل امنیت لایه بندی شده، مربوط به ابزار منفرد مانند سرورها، کامپیوترهای شخصی، سوئیچ ها، روترها و غیره در شبکه ا ست. هر ابزار تعدادی پارامتر قابل تنظیم دارد و هنگامی که به نادر ستی تنظیم شوند، می توانند سوراخ های امنیتی نفوذپذیری ایجاد کنند. این پارامترها شامل تنظیمات رجیستری، سرویس ها، توابع عملیاتی روی خود ابزار یا وصله های سیستم های عامل یا نرم افزارهای مهم می شود.

تکنولوژی های زیر امنیت را در سطح میزبان فراهم می کنند:

- IDSهای سطح میزبان: IDSهای سطح میزبان عملیاتی مشابه با IDS های شبکه انجام می دهند؛ تفاوت اصلی در نمایش ترافیک در یک ابزار شبکه به تنهایی است. IDSهای سطح میزبان برای مشخص شدن عملیات بخصوصی از ابزار میزبان تنظیم می گردند و بنابراین اگر به درستی مدیریت شوند، درجه بالایی از مراقبت را فراهم می کنند.
- تابعیت امنیتی کاربر انتهایی: روش های تابعیت امنیتی کاربر انتهایی وظیفه دوچندانی ایفا می کنند و هم شبکه (همانگونه در بخش قبلی مطرح شد) و هم میزبان های جداگانه را محافظت می کنند. این روش ها بطور پیو سته میزبان را برای عملیات زیان ر سان و آلودگی ها برر سی می کنند و همچنین به نصب و به روز بودن فایروال ها و آنتی ویروس ها رسیدگی می کنند.
- آنتی ویروس: هنگامی که آنتی ویروس های مشخص شده برای میزبان در کنار آنتی ویروس های شبکه استفاده می شوند، لایه اضافه ای برای محافظت فراهم می کنند.
- کنترل دسترسی\تصدیق هویت: ابزار کنترل دسترسی در سطح ابزار یک روش مناسب است که تضمین می کند د سترسی به ابزار تنها تو سط کاربران مجاز صورت پذیرد. در اینجا نیز، احتمال سطح بالایی از تراکنش بین ابزار کنترل دسترسی شبکه و کنترل دسترسی میزبان وجود دارد.

۷-۲. مزایا، معایب و ملاحظات سطح میزبان

این تکنولوژی های در سطح میزبان حفاظت بالایی ایجاد می کنند زیرا برای برآورده کردن م شخ صات عملیاتی مخ صوص یک ابزار پیکربندی می گردند. دقت و پا سخ دهی آنها به محیط میزبان به مدیران اجازه می دهد که به سرعت م شخص کنند کدام تنظمیات ابزار نیاز به به روز رسانی برای تضمین عملیات امن دارند.

بکارگیری و مدیریت سیستم های سطح میزبان می تواند بسیار زمان بر باشند. از آنجایی که این سیستم ها نیاز به نمایش و به روز ر سانی مداوم دارند، اغلب ساعات زیادی برای مدیریت منا سب می طلبند. اغلب نصب شان م شکل ا ست و تلاش قابل ملاحظه ای برای تنظیم آنها مورد نیاز است.

همچنین، هرچه سیستم عامل بیشتری در شبکه داشته باشید، یک رویکرد برپایه میزبان، گران تر خواهد بود و مدیریت این ابزار مشکل تر خواهد شد. همچنین، با تعداد زیادی ابزار امنیتی سطح میزبان در یک شبکه، تعداد هشدارها و علائم اشتباه می تواند بسیار زیاد باشد. بدلیل هزینه ها و باراضافی مدیریت، ابزار در سطح میزبان باید بدقت بکار گرفته شوند.

۸. سطح ۴: امنیت برنامه کاربردی

در حال حاضر امنیت سطح برنامه کاربردی بخش زیادی از توجه را معطوف خود کرده است. برنامه هایی که به میزان کافی محافظت نشده اند، می توانند دسترسی آسانی به دیتا و رکوردهای محرمانه فراهم کنند .حقیقت تلخ این است که بیشتر برنامه نویسان هنگام تولید کد به امنیت توجه ندارند .این یک مشکل تاریخی در بسیاری از برنامه های با تولید انبوه است. ممکن است شما از کمبود امنیت در نرم افزارها آگاه شوید، اما قدرت تصحیح آنها را نداشته باشید.

برنامه ها برای دستر سی مشتریان، شرکا و حتی کارمندان حاضر در محل های دیگر، روی وب قرار داده می شوند .این برنامه ها، همچون بخش فروش، مدیریت ارتباط با مشتری، یا سیستم های مالی، می توانند هدف خوبی برای افرادی که نیات بد دارند، باشند .بنابراین بسیار مهم است که یک استراتژی امنیتی جامع برای هر برنامه تحت شبکه اعمال شود.

تکنولوژی های زیر امنیت را در سطح برنامه فراهم می کنند:

- پوشش محافظ برنامه: از پوشش محافظ برنامه به کرات به عنوان فایروال سطح برنامه یاد می شود و تضمین می کند که تقاضاهای وارد شونده و خارج شونده برای برنامه مورد نظر مجاز هستند. یک پوشش که معمولاً روی سرورهای وب، سرورهای ایمیل، سرورهای پایگاه داده و ماشین های مشابه نصب می شود، برای عملکرد مورد انتظار سیستم میزبان تنظیم می گردد و با درجه بالایی با سیستم یکپارچه می شود.
- کنترل دستر سی/تصدیق هویت: مانند تصدیق هویت در سطح شبکه و میزبان، تنها کاربران مجاز می توانند به برنامه دسترسی داشته باشند.
- تعیین صحت ورودی: ابزارهای تعیین صحت ورودی بررسی می کنند که ورودی گذرنده از شبکه برای پردازش امن باشد. اگر ابزارهای امنیتی مناسب در جای خود مورد استفاده قرار نگیرند، هر تراکنش بین افراد و واسط کاربر می تواند خطاهای ورودی تولید کند. عموماً هر تراکنش با سرور وب شما باید ناامن در نظر گرفته شود مگر اینکه خلافش ثابت شود! به عنوان مثال، یک فرم وبی با یک بخش برای ورود برای کد پستی را در نظر بگیرید. ورودی قابل پذیرش در این قسمت فقط ده کاراکتر عددی است.

۸-۲. مزایا، معایب و ملاحظات سطح برنامه

ابزارهای امنیت سطح برنامه موقعیت امنیتی کلی را تقویت می کنند و به شما اجازه کنترل بهتری روی برنامه هایتان را می دهند. همچنین سطح بالاتری از جوابگویی را فراهم می کنند چرا که بسیاری از فعالیت های نمایش داده شده توسط این ابزارها، ثبت شده و قابل ردیابی هستند.

اما در عوض پیاده سازی جامع امنیت سطح برنامه می تواند هزینه بر باشد، چرا که هر برنامه و میزبان آن باید بصورت مجزا ارزیابی، پیکربندی و مدیریت شود. بعلاوه، بالابردن امنیت یک شبکه با افزایش صرف امنیت سطح برنامه نمی تواند امنیت کامل را تضمین کند. هرچه زودتر بتوانید سیاست هایی برای استفاده از این ابزارها پیاده کنید، روند مذکور موثرتر و ارزان تر خواهد بود.

ملاحظات کلیدی برنامه ها و طرح های شما را برای بلندمدت اولویت بندی می کنند. امنیت را روی برنامه ها کاربردی خود در جایی پیاده کنید که بیشترین منفعت مالی را برای شما دارد. طرح ریزی بلند مدت به شما اجازه می دهد که ابزارهای امنیتی را با روشی تحت کنترل در طی رشد شبکه تان پیاده سازی کنید و از هزینه های اضافی جلوگیری می کند.

۹. سطح ۵ : امنیت دیتا

امنیت سطح دیتا ترکیبی از سیا ست امنیتی و رمزنگاری را دربرمی گیرد. رمزنگاری دیتا، هنگامی که ذخیره می شود و یا در شبکه شما حرکت می کند، به عنوان رو شی بسیار منا سب تو صیه می گردد، زیرا چنانچه تمام ابزارهای امنیتی دیگر از کار بیفتند، یک طرح رمزنگاری قوی دیتای مختص شما را محافظت می کند.

امنیت دیتا تا حد زیادی به سیا ست های سازمانی شما وابسته ا ست. سیا ست سازمانی می گوید که چه کسی به دیتا دسترسی دارد، کدام کاربران مجاز می توانند آن را دستکاری کنند و چه کسی مسوول نهایی یکپارچگی و امن ماندن آن است. تعیین صاحب و متولی دیتا به شما اجازه می دهد که سیا ست های د ستر سی و ابزار امنیتی منا سبی را که باید بکار گرفته شوند، مشخص کنید.

تکنولوژی های زیر امنیت در سطح دیتا را فراهم می کنند:

- رمزنگاری: طرح های رمزنگاری دیتا در سطوح دیتا، برنامه و سیستم عامل پیاده می شوند. تقریباً تمام طرح ها شامل کلیدهای رمزنگاری/ رمزگشایی هستند که تمام افرادی که به دیتا د ستر سی دارند، باید دا شته با شند. استراتژی های رمزنگاری معمول شامل PKI[۱] ، RSA[۲] و ... می باشند.[۱۲]
- کنترل دسترسی / تصدیق هویت: مانند تصدیق هویت سطوح شبکه، میزبان و برنامه، تنها کاربران مجاز دسترسی به دیتا خواهند داشت.

۹-۱. مزایا، معایب و ملاحظات سطح دیتا

رمزنگاری روش اثبات شده ای برای محافظت از دیتای شما فراهم می کند. چنانچه نفوذگران تمام ابزارهای امنیتی دیگر در شبکه شما را خنثی کنند، رمزنگاری یک مانع نهایی و موثر برای محافظت از اطلاعات خصوصی و دارایی دیجیتال شما فراهم می کند.

از سوی دیگر بار اضافی برای رمزنگاری و رمزگشایی دیتا وجود دارد که می تواند تأثیرات زیادی در کارایی بگذارد. به علاوه، مدیریت کلیدها می تواند تبدیل به یک بار اجرایی در سازمان های بزرگ یا در حال رشد گردد.

رمزنگاری تا عمق مشخص باید به دقت مدیریت شود. کلیدهای رمزنگاری باید برای تمام ابزارها و برنامه های تحت تأثیر تنظیم و هماهنگ شوند. به همین دلیل، یک بار مدیریتی برای یک برنامه رمزنگاری موثر مورد نیاز است.

۱۰. نتیجه گیری

در قسمت های قبل به لایه های مختلف در امنیت لایه بندی شده شبکه و معایب، مزایا و ملاحظات هر لایه پرداختیم. در این قسمت به اختصار به جمع بندی مباحث فوق می پردازیم. مباحث گذشته نشان می دهد که چگونه رویکرد امنیت لایه بندی شده در مقابل تهدیدها و حملات معمول از شبکه شما محافظت می کند و نشان می دهد که چگونه هر سطح با داشتن نقشی کلیدی در برقراری امنیت شبکه جامع و مؤثر، شرکت می کند.

هکرها و تروریست های فضای سایبر به طور فزاینده ای اقدام به حمله به شبکه ها می کنند. رویکرد سنتی به امنیت یعنی یک فایروال در ترکیب با یک آنتی ویروس در محافظت از شما در برابر تهدیدهای پیشرفته امروزی ناتوان است.

---

[۱] Public Key Infrastructure
[۲] Rivest Shamir Adelman

اما شما می توانید با برقراری امنیت شبکه با استفاده از رویکرد لایه بندی شده دفاع مستحکمی ایجاد کنید. با نصب گزینه شی ابزارهای امنیتی در پنج سطح موجود در شبکه تان (پیرامون، شبکه، میزبان، برنامه و دیتا) می توانید از دارایی های دیجیتالی خود محافظت کنید و از افشای اطلاعات خود در اثر ایجاد رخنه های مصیبت بار تا حد زیادی بکاهید.

مراجع

[۱] – حسین شیرازی، رحمت اله امیر صوفی و دیگران، ۱۳۹۰ ، ارائه طرح معماری جنگ اطلاعات، فصلنامه علمی پژوهشی مدیریت نظامی، شماره ٤٢ ، سال یازدهم ، صفحه ۱۲۲-۱٤٦

[۲] – محمد خالقی، سند راهنمای پیاده سازی سیستم مدیریت اطلاعات، دبیرخانه شورای عالی امنیت فضای تبادل اطلاعات، ۱۳۸۳

[۳]- سعید قنبري، پیاده سازي سیستم مدیریت امنیت اطالعات مبتني بر استاندارد BS۷۷۹۹ در یک سازمان فرضي با تاکید بر ارزیابي مخاطرات، پایان نامه مقطع کارشناسي ارشد،دانشگاه صنعتي مالک اشتر، ۱۳۸۵.

[٤]- ISMS Implementation Guide, By Vinod Kumar Puthuseeri, ۲۰۰٦; http://www.infosecwriters.com/text_resources/p df/ISMS_VKumar.pdf

[٥] - ابراهیم محمود زاده، مهدي رادرجبي، مدیریت امنیت در سیستم هاي اطالعاتي، فصلنامه علوم مدیریت ایران ، دوره اول ، شماره ی ٤ ، زمستان ۱۳۸٥

[٦] - Active Audit Agancy, Road map for ISO ۲۷۰۰۱ implementation, http://www.auditagency.com.ua/?r=blog_۱٤_Ro adMap

[۷] - International Organization for Standardization, List of ISO technical committees, http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees.htm

[۸] - ISO/IEC ۲۷۰۰۱ :۲۰۰٥ (BS ۷۷۹۹-۲: ۲۰۰٥) Information technology – Security techniques – Information security management systems – Requirements

[۹]- Maximus International LLC, ISMS Lead Auditor Course, Training Material, ۲۰۱۰

[۱۰] - Thomas M Thomas II, Thomas M. Thomas, Donald Stoddard, “Network Security First-Step “, Cisco Press,۲۰۱۱.

[۱۱] - John R. Vacca, “Network and System Security”, first edition, Syngress,۲۰۱۰

[۱۲] - William Stallings, “Cryptography and Network security: principals and pracice”, fifth edition, Pearson, ۲۰۱۱